cryptography

MDPI

Article

QUARC: Quantum Research Cubesat—A Constellation for Quantum Communication

Luca Mazzarella [1,*,†], Christopher Lowe [2], David Lowndes [3], Siddarth Koduru Joshi [3], Steve Greenland [4], Doug McNeil [4], Cassandra Mercury [4], Malcolm Macdonald [2], John Rarity [3] and Daniel Kuan Li Oi [1]

1 SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK; daniel.oi@strath.ac.uk
2 Department of Mechanical and Aerospace Engineering, University of Strathclyde, Level 8, James Weir Building, 75 Montrose Street, Glasgow G1 1XJ, UK; christopher.lowe@strath.ac.uk (C.L.); malcolm.macdonald.102@strath.ac.uk (M.M.)
3 Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK; david.lowndes@bristol.ac.uk (D.L.); sk.Joshi@bristol.ac.uk (S.K.J.); john.rarity@bristol.ac.uk (J.R.)
4 Craft Prospect ltd. Tontine building, 20 Trongate, Glasgow G1 5ES, UK; steve@craftprospect.com (S.G.); doug@craftprospect.com (D.M.); cassandra@craftprospect.com (C.M.)
* Correspondence: luca.mazzarella@jpl.nasa.gov
† Current address: Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, MS 298-102, Pasadena, CA 91109, USA.

Received: 23 December 2019; Accepted: 21 February 2020; Published: 27 February 2020

Abstract: Quantum key distribution (QKD) offers future proof security based on fundamental laws of physics. Long-distance QKD spanning regions such as the United Kingdom (UK) may employ a constellation of satellites. Small satellites, CubeSats in particular, in low Earth orbit are a relatively low-cost alternative to traditional, large platforms. They allow the deployment of a large number of spacecrafts, ensuring greater coverage and mitigating some of the risk associated with availability due to cloud cover. We present our mission analysis showing how a constellation comprising 15 low-cost 6U CubeSats can be used to form a secure communication backbone for ground-based and metropolitan networks across the UK. We have estimated the monthly key rates at 43 sites across the UK, incorporating local meteorological data, atmospheric channel modelling and orbital parameters. We have optimized the constellation topology for rapid revisit and thus low-latency key distribution.

Keywords: SatQKD; CubeSats; satellite constellations

1. Introduction

Encryption is vital for securing the transmission of personal, commercial and governmental data. The rapid development of quantum computation threatens the underpinnings of current public key cryptographic methods, most notably the RSA (Rivest–Shamir–Adelmann) cryptosystem [1], that are the basis of the internet. Hence, there is the need for the development of "quantum-safe" communication methods that can provide forward security for critical information. We also note the development of "post-quantum cryptography" [2] that seeks replacement public key algorithms that are resistant to attack by quantum and classical computers. Quantum key distribution (QKD) has been proposed as a solution that allows two distant parties—traditionally named Alice and Bob—to establish a joint secret key of which the security is dependent not on computational complexity assumptions but on the laws of quantum physics. There has been significant effort toward its theoretical and experimental development [3–6] over more than three decades, with commercial fibre-based systems now commercially available. However, fibre losses scale exponentially with distance, greatly restricting

the range of terrestrial QKD. Conventional optical repeaters cannot be used with QKD [7–9] since quantum information cannot be perfectly and deterministically copied [10,11] and practical quantum memories are still a long-term prospect. Satellites are currently the only viable option for extending QKD communication ranges beyond distances greater than a few hundred kilometers [12–16] and thus for enabling the global quantum internet [17].

In this article, we present an overview of the quantum research CubeSat (QUARC) space mission and evaluate the feasibility of providing a secure satellite quantum key distribution (SatQKD) service to the UK via a constellation of CubeSats. Another recent work on satellite constellations for QKD networks but with different aims can be found in Reference [18]. Recently, Satellite quantum communication has witnessed an unprecedented growth including proof-of-principle experiments [19–25], quantum mechanics fundamental tests [26,27], and the launch and operation of a QKD satellite [28–30]. These groundbreaking results have spurred an international space race involving university consortia, national agencies and private companies, e.g., QKDSat (ArQit) [31], QUARTZ (SES) [32], QEYSSAT (Canada) [33], UK–Singapore Bilateral (RAL Space—CQT) [34], QUBE (Deutsches Zentrum für Luft- und Raumfahrt (DLR) + German Universities) [35], NANOBOB (Austria–France) [36] and IOD-6/ROKS (UK) [37]. Many of these efforts focus on satellites belonging to the domain of large and complex platforms, and little research has been carried out so far regarding QKD performance evaluation using smaller satellites. On the other hand, Small Satellites (SmallSats) and especially the popular CubeSat standard have been in the spotlight for their potential to deliver meaningful communication volumes at a significantly reduced price and complexity. Operationally, they represent a path finder option for the deployment of large constellations offering rapid revisit and therefore greater coverage than a single large spacecraft [38,39].

The objective of the QUARC space mission is to provide a QKD service to a specific region: the UK. We identify relationships between satellite constellation topology, the atmospheric channel and historical weather data and estimate key rates over 43 ground stations (gateways) uniformly distributed across the UK (Figure 1) serviced by a constellation of 15 satellites. These gateway locations cannot be connected currently via the installed fiber network, and they have been defined specifically in order to gain an understanding of how communication performance varies across different regions at different times throughout the year. The aim is not to satisfy a particular revisit/coverage requirement but to offer a generalised performance metric from which performance can be scaled by the number and location of gateways and by the number and distribution of satellites in the constellation. More satellites result in a greater level of expected coverage and secure key, while more gateways result in a higher probability of contact being made and a smaller amount of key data being received at each individual gateway. Here, we have chosen not to focus on the key management and scheduling problems but we refer the reader to recent works on these topics [40,41].

The number of keys that can be distributed between the constellation and each gateway throughout the year is evaluated via simulation that incorporates effects from cloud cover, sunrise/sunset, and various sources of losses and spurious counts in order to consider the impact of the changing seasons and latitude. The best case scenario is found to be represented by the southeast England gateway where $\sim$ 300 kbit/night/satellite of key can be exchanged during August, while the worst case is represented by the northeast islands of Scotland, where no key can be distributed; this is due to the constraint of nighttime operations that we have assumed for the purposes of the analysis. We assume a conservative level of system performance and that daytime background light would result in excessive spurious counts, curtailing operations. We also conservatively assume that QKD operations are not possible in twilight or dusk conditions. In practice, some nonzero key rates may be possible with small levels of background light and a more detailed simulation incorporating site-level background light and astronomical data, e.g., position of the moon, is in development. SatQKD systems that can operate in daytime are currently under development by various groups [42–45] but not yet fully demonstrated in orbit. On the other hand, when the constellation is required to distribute keys not only to a single gateway but also to all gateways, the best case scenario secret key volume

decreases to 160 kbit/night/satellite, which is also in southeast England. Our results indicate that a CubeSat constellation has the potential to deliver a meaningful amount of secret key for scenarios requiring small-volume, highly secure communication via quantum-resistant symmetric key ciphers like Advanced Encryption Standard (AES) [46]. We have also carried out preliminary system design and tests of the payload acquisition, pointing and tracking (APT) system, which is a vital subsystem for long-distance free-space QKD; these will be detailed in a separate paper.

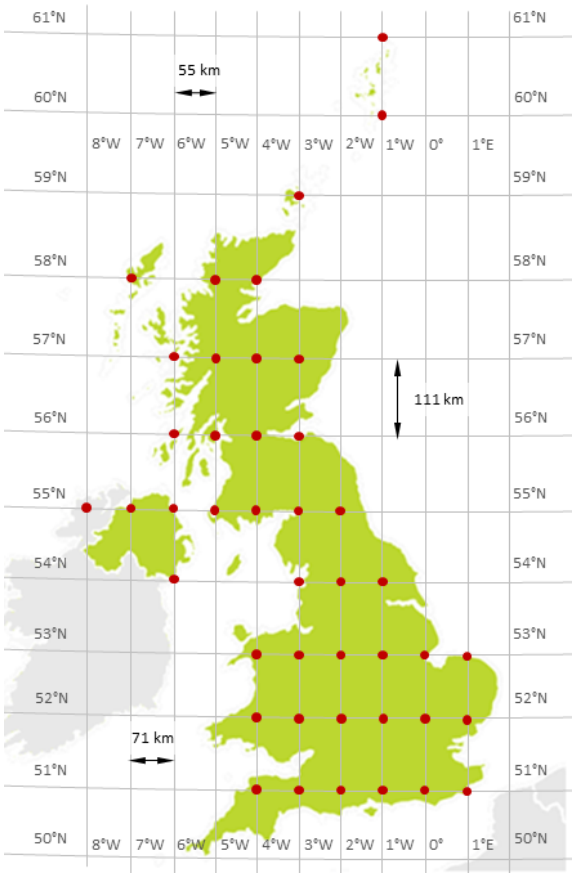

Figure 1. Distribution of 43 hypothetical gateways (red dots) distributed across the UK region.

The rest of this work is structured as follows: In Section 2, we outline the payload design, in particular the acquisition pointing and tracking system. In Section 3, we describe the model for the quantum channel. In Section 4, we present the mission design and discuss the orbital choice for the satellite constellation. In Section 5, we model the key exchange between the constellation and the set of gateways. Section 6 is devoted to the presentation of the mission performance. Finally, this paper concludes with Section 7.

2. Payload Design and System Outline

This section gives a brief description of the QKD payload and subsystems used in the mission analysis. A concept outline for the 6U CubeSat is shown in Figure 2. Such a payload has similarity to free-space optical communication payloads in development for nanosatellite missions [35,36,47] and handheld devices [48,49]. SatQKD can be divided into two main types: untrusted and trusted node [12]. Untrusted node SatQKD ensures verifiable security between two grounds stations via Bell test measurements without any assumption of the security of the satellite itself. This requires simultaneous links between the satellite and the two ground stations, difficult to achieve with high key rates. On the other hand, the trusted node paradigm assumes the satellite to be outside the domain of influence of an eavesdropper. For near-term realisation of SatQKD, the trusted node scenario

is thus the most feasible. Trusted node SatQKD can be realised using the spacecraft as a receiver (uplink (UL) configuration) or as a transmitter (downlink (DL) configuration). A DL configuration requires the development of a space-qualified optical assembly for precise pointing of the order of few μrad and quantum sources driven by quantum random number generators [38,39]. The UL configuration requires a less complicated payload comprising single photon detectors but would also require a larger telescope compared to DL [36,47]. However, in this configuration, the upward beam encounters turbulence early during its path, leading to larger path deviations (the so-called shower curtain effect) and therefore higher losses, on the order of 20 dB greater with respect to the DL configuration [12,16,50,51]. In this work, we therefore focus attention on the DL scenario.

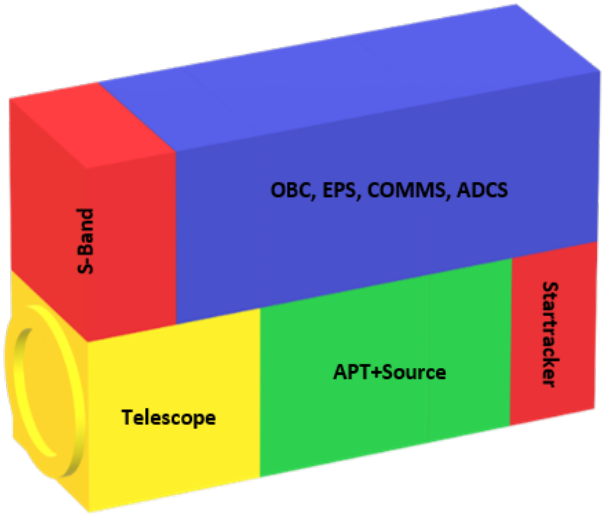

Figure 2. Layout of 6U CubeSat: Approximately 3U (2.5 litres) of volume is reserved for the platform systems including the electrical power system (EPS), communications (COMMS), on-board computer (OBC) and attitude determination and control system (ADCS). The ADCS incorporates a star tracker (shown separately) to provide sub-0.25° coarse pointing and is located on the opposite face to the transmission aperture. The transmission telescope occupies 1U, the source and APT system occupy 1.5U and the payload electronics occupy 0.5U. An S-band antenna is located on the same face as the transmission telescope to allow high-speed radio frequency (RF) communications during the QKD pass for real-time data post-processing. The satellite bus would also include deployable solar panels to recharge on-board batteries that would provide sufficient power for repeated QKD operations during the eclipse phase of the orbit. Appropriate 6U CubeSat buses are available from commercial providers such as Blue Canyon Technologies (www.bluecanyontech.com), Endurosat (www.endurosat.com), GomSpace (gomspace.com), Innovative Solutions In Space (www.isispace.nl) and AAC Clyde Space (www.aac-clyde.space).

Quantum Source: QKD requires the ability to send extremely faint pulses of light at a high repetition rate and with a polarization randomly selected from a set of non-orthogonal signal states. This can be achieved by combining multiple differently polarized sources or by modulating the polarization of a single source. Currently, we plan to use multiple polarized LEDs (extinction 1000:1) combined with a single-mode fibre to remove spatial information. LEDs have a wide spectrum, and therefore with appropriate filtering, they are resilient to mismatches in wavelengths between the LEDs. Recent advances in integrated optics could also be leveraged using interferometers to modulate light and 2D grating couplers to generate the polarization states from a single source [52]. An integrated platform would be smaller but would require additional hardware to monitor the output. Such sources have been previously developed with small size, weight and power (SWaP) envelopes of the orders of $10^{-4}m^3$, 10^{-1} kg and < 1 W. They can be made to be monolithic, solid-state devices with further miniaturisation possible through integrated optics fabrication [53,54]; hence, the source can

be accommodated in 1U. The main issues will be wavelength matching between different emitters to prevent side-channel leakage, modest temperature stability and reliability in the space environment; the latter is still to be proven [55].

For the source wavelength, we have chosen 808 nm for ease of laser diode selection, atmospheric transmission and low background light during night operations due to atmospheric scattering of moonlight and OH recombination in the upper atmosphere [56]. We assume a pulse repetition rate of 100 MHz, comparable with QUESS/Micius [28]) and quite modest compared to what is currently achievable in fiber [57].

An important aspect of such a source is a supply of truly random and securely generated bits. For a 2-Decoy State Protocol, 4 bits per pulse need to be generated at a rate of 400 Mbps, leading to several tens of gigabytes of random data required for a single pass. For protocols requiring biased basis and signal choices, this will increase the required generation rate. High speed quantum random number generators (QRNGs) with suitable SWaP requirements exist, allowing real-time on-the-fly provision though in-orbit demonstration and validation are still required [58]. A QKD protocol also requires bidirectional classical communication between Alice and Bob for reconciliation, error correction and privacy amplification which can be performed by RF communications over public channels.

Acquisition, Pointing and Tracking System: In low earth orbit (LEO), the transmission range varies from a few hundred km at zenith up to about 2000 km at low elevations. It is therefore crucial to achieve a pointing accuracy of the order of micro-radians in order to mitigate channel losses. In our system, pointing is achieved in two stages: coarse pointing and fine pointing.

The coarse-pointing stage is provided by pointing the body of the satellite via ADCS and hence the rigidly mounted telescope. Fine pointing is provided by a closed-loop beam steering system using a beacon tracking camera (BTC) and a MEMS micromirror (MM) (Figure 3). A MM is a mirror that can be tilted independently over the x and y axes. We have chosen a Mirrorcle S40069 [59] that has a 5-mm diameter and can be mechanically tilted to up $\pm 5^{\circ}$ (optical tilt $\pm 10^{\circ}$) with step of 1.3 μrad (the transmission telescope magnification improves this precision by a factor of 30) and is controlled using a software proportional-integral-differential (PID) controller. The quantum signal and both UL and DL beacons are co-aligned on the main boresight of the telescope through in-orbit calibration; these are steered by the MM driven by the output of the BTC. A DL beacon is sent at 905 nm and is coupled into the beam path by a short-pass dichroic mirror, co-aligned with the 808-nm quantum signal. The DL beacon also carries a clock signal synchronised with the 808-nm quantum signal pulses, allowing the optical ground station (OGS) to perform coincidence matching and background event rejection. The UL beacon—chosen to be at 850 nm—is picked out of the beam path by a short-pass dichroic. The image of the UL beacon is focused onto the UL Beacon Camera which is read out at up to 1 kHz in the region-of-interest mode. Preliminary testing indicates that $\sim$ μrad pointing precision is achievable with modest UL beacon power with careful optimisation of the centroiding algorithm parameters.

The field of view (FoV) of the UL beacon camera is 5.5 mrad, compared with the telescope FoV 17.5 mrad (Figure 4). Hence, it is simple to scan the entire telescope FoV using the MM beam steering function for initial acquisition of the UL beacon. In this mode, the beacon spot is simply required to be guided close to the set point; this can be achieved in the time or order of 1 second. After this has been achieved, only a small fraction of the camera sensor needs to be read, which speeds up the tracking loop by up to an order of magnitude.

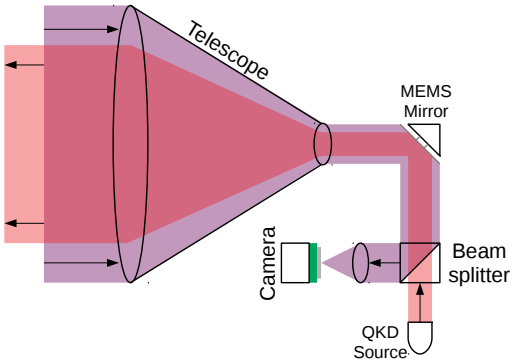

Figure 3. Downlink fine-pointing system schematic: A 90-mm telescope collects light from a beacon on the optical ground station (OGS) and produces a collimated 3-mm beam that reflects off a micro-electromechanical system (MEMS) mirror that provides beam steering. The beacon light is separated on a dichroic beamsplitter and is directed towards the beacon camera. The beacon spot position on the sensor is used as a feedback signal to the MEMS mirror to correct errors in satellite pointing. The QKD source is coupled into the other arm of the beamsplitter so that the QKD and beacon beams are nominally colinear and counterpropagating. Due to the rapid transverse motion of the satellite and the small transmitted beam divergence, a point ahead correction is required. The DL beacon has been omitted for clarity. A second dichroic mirror combines the DL beacon with the outgoing quantum signal. This allows the OGS to track the satellite as well as to convey precise timing and synchronisation information required to pick out the faint quantum signals from background noise.

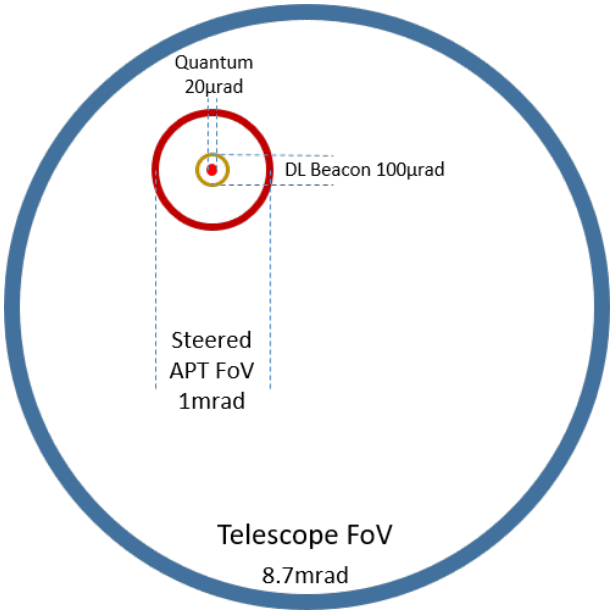

Figure 4. Fields of view: The telescope has a $\pm 0.25^\circ = 4.36$ mrad half FoV to match the coarse-pointing performance of a moderate ADCS system. The effective MM steerable range is $\pm \frac{10^\circ}{30} = 0.33^\circ$. The FoV of the uplink beacon camera is 1 mrad as this is restricted by packaging constraints of the optical path and component sizes; in principle, this could be up to ± 5 based on the UL beacon pixel array size. The DL beacon has a divergence of 100 μrad, wider than the 20-μrad beam width of the quantum signal to ensure that timing and synchronisation are still maintained in the event of temporary fine-pointing excursion beyond the quantum beam width.

Once UL beacon lock has been achieved by the fine-pointing mechanism, the deviation of the MM from the neutral position represents a boresight error and this can be fed back to the ADCS to improve coarse pointing. This would allow the reduction of the required telescope FoV that is diffraction

limited; degraded performance of the outer field is acceptable for initial UL beacon acquisition, and the use the fine-pointing feedback signal to the ADCS would greatly reduce the coarse-pointing error so that quantum transmission would be restricted to a central region of the telescope FoV.

The centroid position of the beacon is compared with a set-point. The set-point includes a point-ahead offset that depends on the transverse velocity of the satellite with respect to the OGS-satellite line-of-sight (LoS) that can reach a maximum of 50 μrad; this can precomputed as a function of time during the pass. A correction signal is sent to the MM driver that performs beam steering so that the UL beacon spot is brought towards the set-point. Our preliminary implementation shows that the APT systems should occupy no more that 1U.

Transmission optics: The transmission optics is specified as a 30× telescope of 90-mm diameter (Figure 5). The exit pupil position, where the MM will be placed (back-focus position), and the size of the rear element should be compatible with the APT system geometry. The telescope should be athermal for the range of temperatures of operation, nominally 20 °C to +30 °C, and should be achromatic over the wavelength range 800 nm to 850 nm. The optics should be polarisation insensitive along the (transmissive) quantum signal beam path. A maximum volume of 2U is specified for the transmission optics; this should be achievable with a reflective or catadioptric design, and its mass should be below 2kg.

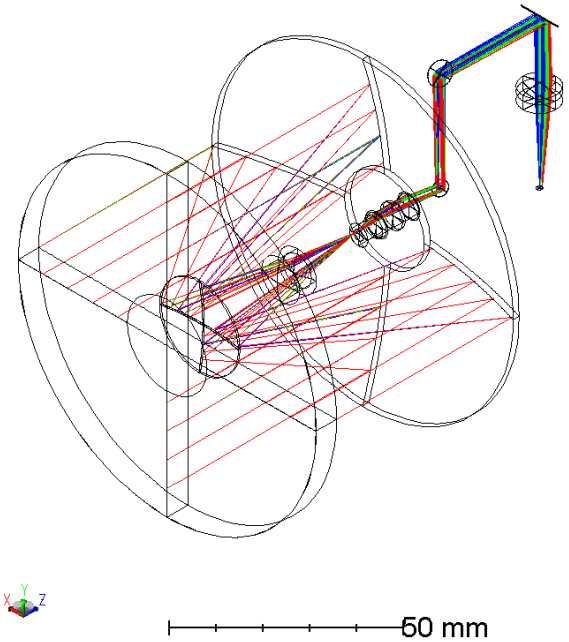

Figure 5. Preliminary payload telescope and beacon camera optical design concept: The 90-mm diameter 30× afocal catadioptric telescope has diffraction-limited performance between 800–850 nm over a field of view of ±0.25° and is 75 mm long. The MM (fast steering mirror) is located at the exit pupil to the rear of the telescope. Incoming uplink beacon light is directed to the uplink beacon camera via a fold mirror, dichroic mirrors and a focusing lens. The dichroic mirrors combine the outgoing quantum signal and downlink beacon (neither are shown).

In summary, a 6U CubeSat is proposed for the QUARC mission, which comprises approximately 2U of volume for the APT and source, 2U of volume for the telescope system and 2U of volume for the supporting platform systems. The supporting systems not only must carry out housekeeping operations such as power management, command and data handling, and telecommunications to traditional ground stations but also must take care of advanced functions such as coarse pointing via an ADCS and orbit station-keeping using a propulsion system. Orbit station keeping is required to

maintain precise Earth and Sun synchronisms, without which the repeat ground track characteristics would quickly be lost, sacrificing targeted coverage over the chosen region. This will be further discussed in Section 4.

3. Channel Analysis

Losses as well as spurious counts are detrimental for the final secret key rate as it makes the quantum state less distinguishable [11,60]. In this section, we are going to model the channel between the satellite and the OGS and to review the source of losses and background counts. The physical scenario is summarized in Figure 6.

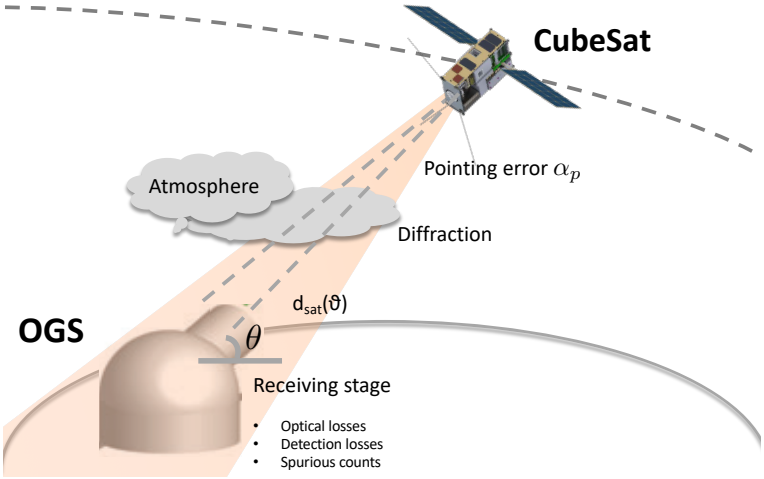

Figure 6. Quantum channel representation: In modelling the quantum channel, we have considered various source of losses, spurious counts and source errors, all of which decrease the final secret key rate.

3.1. Channel Losses

Diffraction: Losses due to diffraction of the transmitted beam over the distance between satellite and OGS are by far the most important losses. The distance depends on the orbital altitude and on the elevation of the satellite, as seen by the OGS. In this proposed mission, we consider a circular orbit with an altitude of 574 km; the distance between the satellite and the OGS will thus range between 574 km—at Zenith—and approximately 1500 km at an elevation of 15° above the horizon.

The full divergence of the beam is $\omega_{div} = 22\,\mu$rad (first minima of the far-field airy distribution assuming a flat-top transmission intensity). If we denote the transmitter (receiver) aperture with D_T (D_R) and with R_θ—the range between the satellite and the OGS for a certain elevation θ—diffraction loss for a beam propagating in the vacuum is given by the following [61]:

$$T_\theta^{Diff} = -20 \log \frac{D_R}{D_T + \omega_{div} R_\theta},$$

The latter expression implies a quadratic increase of losses with the distance travelled by the optical beam. We assume a transmitter aperture of 90 mm and a receiver aperture of 700 mm. The transmitter aperture value is the maximum that can be accommodated in a 6U satellite without the use of deployable optics. The receiver aperture is comparable to the 600-mm primary mirror of the transportable optical ground station developed by DLR for downlink optical communication [62]. Furthermore, commercial, off-the-shelf (COTS) 700-mm telescope systems are available from companies such as PlaneWave [63] that are purposed for satellite laser communications [64].

Atmospheric Losses: The atmospheric losses are due to scattering and absorption from the atmospheric constituents, and they are relevant only within 20 km from the ground, above which the atmosphere is extremely rarefied. Atmospheric losses depend on the incident wavelength and,

being linked to the path travelled by light, on the elevation angle. This behaviour is captured by the following Equation [65]:

$$T_{\theta}^{Atm} = T_{\lambda} \csc \theta, \tag{1}$$

linking atmospheric losses and elevation angle. T_{λ} is the vertical transmissivity, which is dependent on the signal wavelength and, in the case of 808 nm, is 0.77. The atmospheric transmissivity decreases to 0.5 at 15° elevation [66].

Transmission Pointing Error. As pointed out in Section 2, an increase in pointing error, α_p, increases losses. For a certain beam divergence, ω_{div}, the point error relates to losses via the following relation [50,65]:

$$T_p = e^{-8\alpha_p^2/\omega_{div}^2}, \tag{2}$$

In the current simulation, we assume a pointing error of 1 μrad, leading to a transmissivity of approximately 0.9. Field trial results indicate that this target precision should be possible with further development of our system. It is worth noting that relaxing the pointing requirement to 5 μrad would induce 7 dB extra loss.

Turbulence. Turbulence is a major issue for all free-space optical communication as it causes time and spatially varying regions of refractive index deviations [56]. Light beams can experience deflection (when the characteristic size of the turbulence is large compared with the beam) and wavefront aberrations (when the converse is true) passing through these regions. The DL configuration experiences comparatively little loss due to turbulence compared with the UL configuration, the so-called shower curtain effect. This is because the DL beam experiences turbulence-induced deflection and aberrations only over the last 20 km of its path when its size is much larger than the turbulent eddies; its centroid is thus not going to be displaced significantly. UL beams suffer 10–20 dB more turbulence-induced loss by comparison, as any deflections induced at the start of their path cause large errors at the position of the satellite [50,51,56].

Optics Efficiency. Absorption for the transmitting optics can be pre-compensated choosing a suitable laser intensity as we assume that the satellite is not under the control of a third malicious party. As for the receiving optics, in a standard BB84 setting, a received photon will traverse two beamsplitter; we assume a 50 % transmissivity per optical element.

Detection Efficiency. We assume the use of conventional Si-avalanche photo-diodes (APDs) with standard 40 % quantum efficiency (QE); this value is consistent with that of COTS devices, and this could be improved by using superconducting nanowire single photon detectors (SNSPDs) but at greater expense and SWaP, albeit on the ground [67].

In Figure 7, the total channel loss against the elevation angle is plotted beginning at 15°. Total losses range from approximately 47 dB to 35 dB.

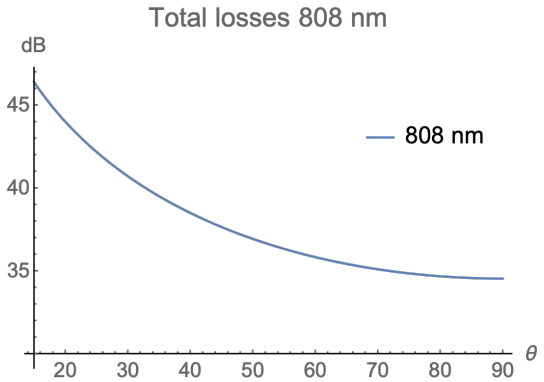

Figure 7. Total losses against elevation angle at 808 nm: This was obtained assuming transmitter and receiver apertures of 90 mm and 700 mm, respectively; beam divergence of 22 μrad; zenith transmissivity of 0.77; pointing error of 1 μrad; optical element transmissivity of 50%; and detection efficiency of 40%. The orbit altitude is assume to be 574 km, and the orbit choice is discussed in Section 4.

3.2. Spurious Counts

Spurious counts are due to electronic noise (dark counts), stray light coming either from the sky or from the environment surrounding the OGS, and polarisation basis errors. The former two sources can be reduced by time filtering the detection counts to narrow coincidence windows around the expected time of arrival of the signal pulses. Assuming a 1-ns gating window and a repetition rate of 100 MHz, we have a 1/10 suppression factor for dark counts.

Detector dark counts: The dark count rate (DCR) of a Si-APDs detector is estimated to be 50 counts per second. This can be improved by using SNSPDs.

Stray light: The stray light contribution to spurious events can also be mitigated by passive spectral filtering; a 1-nm filter (commercially available) effectively eliminates stray light in a rural setting, though it is not as effective in urban areas. Narrower, 0.05-nm filters are also feasible and can in principle enable daylight operation [44]. The Doppler shift of a satellite in LEO is of the order of 0.02 nm; hence, narrower filters would not be suitable unless they could be spectrally tuned during the pass to follow the Doppler shift.

Assuming only nighttime operations and a moonless sky, we have a background count rate on the order of 10^3 counts per second [68]. This may increase by an order of magnitude in the case where a full moon is in the FoV of the OGS.

Polarisation Basis Error: the transmitted and received polarisation bases may be misaligned, leading to detected counts in the wrong channel. We assume a misalignment of 5°.

4. Mission Design

A satellite constellation is proposed, which offers QKD communication through regular, time-critical passes over locations of interest: in this case, the UK. In order to ensure regular coverage without the need for excessive numbers of spacecraft, a Sun and Earth synchronous orbit is proposed. This type of orbit benefits from both consistent illumination conditions over the long term from its Sun synchronism and repeat ground-track properties from its Earth synchronism. A propulsion orbit station-keeping system is required to ensure that such an orbit will be maintained for the duration of a mission. In addition, since a consistent satellite altitude is preferred over the course of the mission, a circular orbit is proposed. Satisfying all of these conditions limits the orbital combinations of altitude and inclination, and for the purposes of the QUARC mission, a repeat ground track after 1 day and 15 orbits is selected. This is achieved with an orbit altitude of 574 km and an orbit inclination of 97.68°.

Constellation Topology. The number and orbital positioning of spacecraft for this mission dictates the level of coverage, which impacts the revisit rate to gateways and thus the communication capacity (ability to transfer data). For example, a single spacecraft would be capable of passing over the UK at most three times per night, with varying levels of elevation above the horizon depending on gateway location. This would not, however, directly translate into multiple key transfer opportunities per night for each gateway due to the fact that communication can only take place between a single satellite–gateway pair at any one time. Therefore, a greater number of spacecrafts would be required to ensure coverage of a greater number of stations, with multiple visits per night. Furthermore, populating multiple orbit planes would enable a distributed revisit schedule over some required period.

In order to obtain regular coverage over the full nighttime period, a constellation of 15 satellites in five orbit planes is proposed and evaluated (Figure 8).

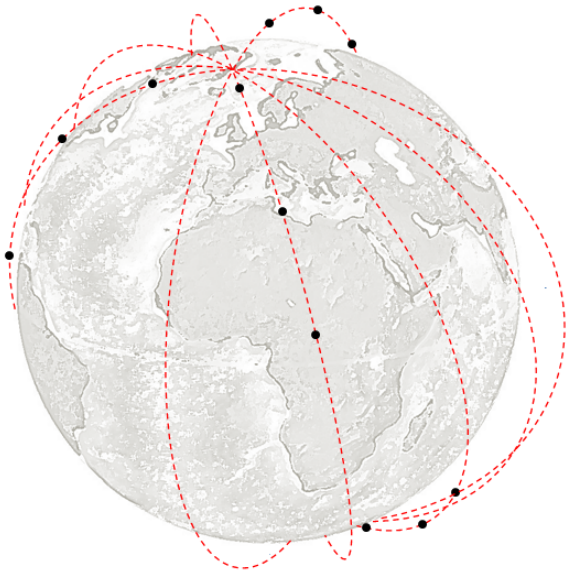

Figure 8. Illustration of satellites (black dots) in the five orbit planes: Note, three of the satellites are out of view in this image, over the far side of the Earth.

The satellites are separated in-plane (difference in true anomaly, TA) by 25° such that passes overhead of a particular ground location occur at intervals of 6 minutes 40 seconds for each of the three-satellite clusters. The orbit planes are separated (difference in Right Ascension of Ascending Node, RAAN) by 30°, which ensures that direct overhead passes occur at 2 hour intervals. Passes with a lower elevation above the horizon, relative to each of the gateways, occur during the orbits preceding and following the overhead pass such that a total of 45 passes are experienced per night from this constellation. A summary of the orbit parameters is shown in Table 1.

Table 1. Constellation topology parameters.

Attribute	Value	Unit	Comment
Orbit Synchronism	Sun & Earth	-	To ensure regular, repeat coverage
Orbit altitude	574	km	-
Orbit inclination	97.68	degrees	-
Orbit eccentricity	0	degrees	Circular, to ensure even coverage
No. orbit planes	5	-	-
No. satellites	15	-	I.e. three satellites per plane
In-plane separation (TA)	25	degrees	Separation between satellites in plane
Cross-plane separation (RAAN)	30	degrees	Separation between planes

The overhead passes are designed to occur at a local time of approximately 20:00 hrs, 22:00 hrs, 00:00 hrs, 02:00 hrs and 04:00 hrs (Figure 8). E.g., the first satellite to pass directly over the UK each night (in the eastern-most plane) should do so early on in the night, while the final satellite to pass directly over the UK (in the western-most plane) should do so in the early hours of the morning. A plot of the elevation angle relative to a point approximately in the centre of the UK (latitude 51.507°, longitude −0.128°) over time is presented in Figure 9, in which the data for each satellite triplet are represented by a different colour and the data for each satellite within each triplet are represented with either a dotted line (first to pass), a dashed line (second) or a continuous line (last in the triplet).

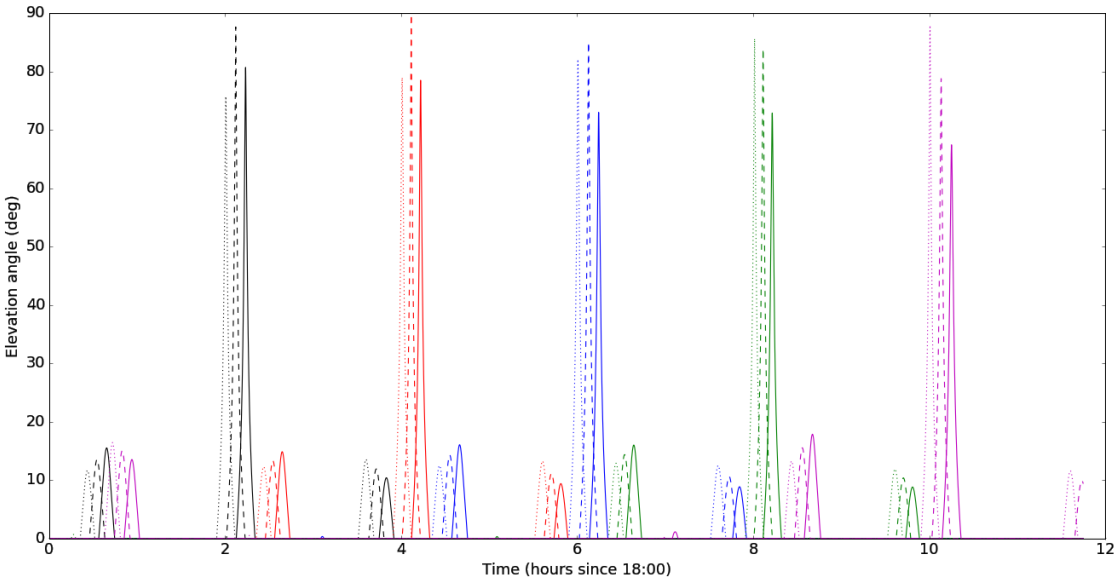

Figure 9. Elevation angle over a central UK gateway for a typical night (time 0 = 18:00): Each colour represents a triplet of satellites (one triplet in each orbit plane). Line-styles represent each satellite in the respective triplets.

Approximately 12 hours after the nighttime ascending passes, there will be a set of associated descending daytime passes, which, while of limited value from a QKD perspective, could offer opportunities for data transfer over traditional (RF) methods of communication. The subsatellite point locations and footprint in which each satellite would be visible is shown in Figure 10 at a time of 00:06:40 hrs.

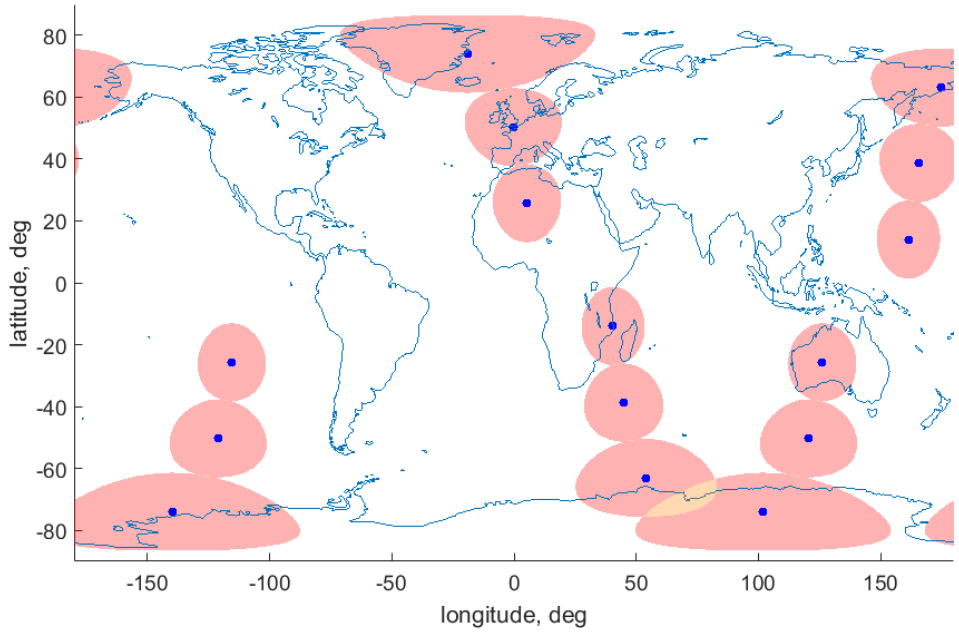

Figure 10. Location of subsatellite points and coverage footprint shortly after midnight.

5. QKD System Performance

True single-photon sources are not a mature technology, yet [69,70], the vast majority of QKD implementations use faint laser pulses. The Poissonian photon statistics of coherent pulse makes them vulnerable to the so-called photon-number-splitting attack. This is where an eavesdropper performs a

weak measurement, selectively blocks all pulses containing a single photon and only resends those containing more than one photon, thus allowing them to have a perfect copy of the exchanged key. This attack can be counteracted by using decoy state methods [71,72], where pulses with different average photon numbers are randomly sent and are used to estimate channel transmissivity and to detect eavesdropper activities. The asymptotic key rate and the quantum bit error rate (QBER) are given by following expressions respectively:

$$K \geq R_r q_f \left(Q_1 (1 - H_2(e_1)) - Q_\mu f_e H_2(e_1) \right), \tag{3}$$

$$E_\mu = \frac{Y_0/2 + e_{det}(1 - e^{-\eta L(\theta)\mu})}{Y_0 + 1 - e^{-\eta L(\theta)\mu}}. \tag{4}$$

where R_r is the repetition rate (100 MHz), q_f is the basis reconciliation factor, f_e is the error correction efficiency, H_2 is the binary entropy, Q_μ is the signal gain (the ratio between the number of events detected by Bob and the number of signals emitted by Alice), Q_1 and E_1 are the estimated gain and the error rate for single photon pulses respectively, and $L(\theta)$ is the loss as a function of the elevation. In what follows, we are going to consider the following parameters: $Y_0 = 10^{-5}$ for the probability of a dark count, $e_{det} = 3.3\,\%$ for the error linked to the stability of the optical system and $\eta = 0.4$ for the detection efficiency. We also consider signal state and decoy state mean photon numbers per pulse of 0.5 and 0.1, respectively. We have chosen fixed values for the intensities; the optimal values depends on the channel conditions but might be hard to compute on the fly. We will leave such optimization as well as the analysis of statistical fluctuation on the key rate for futures works.

QKD requires LoS with a ground station in order to carry out communications; the rate of secret key rate is dependent on the range between the two terminals. As such, in order to maximise key exchange, it is desirable to communicate with ground stations that are directly under the flight path of the satellite: the Zenith condition. This is not always possible due to the nature of orbital mechanics, such that an understanding between the key rate and satellite elevation above the ground terminal's horizon is useful in order to improve the amount of exchanged keys. In a perfect visibility scenario, i.e., no disturbances from the cloud, the following key rates are possible at a wavelength of 808 nm as a function of elevation angle (Figure 11).

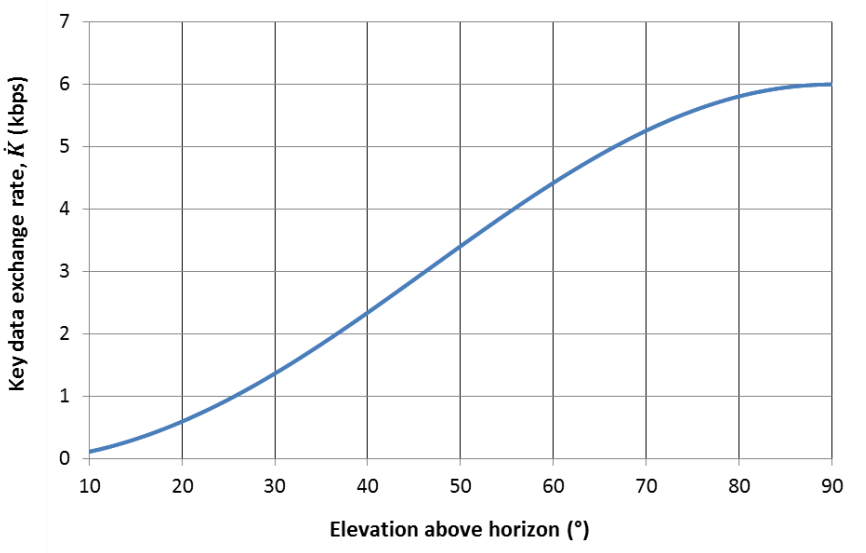

Figure 11. Rate of secure key exchange as a function of elevation.

Ground terminal passes reach various maximum elevations throughout a mission such that the actual number of secure keys exchanged will vary. These are calculated numerically during the

simulation, and the key rate ($\dot{K}$) in bits per second (Figure 10) can be approximated as a 3rd-order polynomial of the elevation angle (θ), using the following equation:

$$\dot{K} = -0.0145\theta^3 + 2.04\theta^2 - 20.65\theta + 88.42. \quad (5)$$

In order to present a real case scenario estimation, we need to consider cloud cover [73], which, if present along the LoS between the spacecraft and ground terminal, prevents any signal transfer.

In order to estimate the probability of LoS between the satellite and gateway, sunshine data is used as a proxy for cloud cover [74]. The primary benefit of this, over direct cloud cover, is that it can be considered a more representative analogy of LoS due to the fact that it is also a measure of a space-borne signal arriving at a ground-based sensor. The data, obtained from the UK Met Office, provides daily averages for the number of sunshine hours at all locations across the UK at a resolution of 5 km $\times$ 5 km [75]. This is provided as an average for each month of the year such that daily or even hourly insights are not obtained. This temporal resolution means that it is not possible to consider different cloud formation effects, e.g., a probability of 50% that the sun is shining does not differentiate between patchy cloud cover over the whole month, complete overcast for half the month and clear skies for half the month, or something in between. The practical implication of this is that these different scenarios will have a different impact on the QKD operations.

Based on an understanding of the day length at various points throughout the year, derived using sunrise and sunset times, it is possible to estimate the average cloud-cover fraction for a specific location. For example, if the time between sunrise and sunset is 12 hours for a certain location in a certain month and the average daily sunshine hours is 6, it can be inferred that there is, on average, 50% cloud cover at that location. It is assumed that this cloud cover approximation remains the same during nighttime hours.

In order to represent the effect of cloud cover on the mission performance, the transfer of keys is modelled such that the key rate is reduced by a fraction equal to the expected level of cloud cover, i.e., a 50% cloud cover will lead to a 50% decrease in the volume of key exchanged. This can be considered a best-case scenario in terms of performance, given that a patchy cloud coverage would impact the performance more than a simple block cloud-coverage scenario.

The time of sunrise and sunset varies significantly throughout the year, and the variation is latitude dependent. The northerly gateways will receive longer dark periods during the winter months and shorter dark periods during the summer months compared to their southerly counterparts. It should be noted that, for the purposes of QKD transmission in this work, sufficient "darkness" is considered to be the time between civil dusk and civil dawn, i.e., when the sun is below the local horizon (elevation angle of less than 0°).

6. Mission Analysis and Results

Analysis of the QUARC mission has been carried out in order to understand the level of performance that could be achieved by a satellite constellation providing QKD services to a UK-wide network of ground-based gateways. Performance, in this case, is defined as the volume of secure key data that could be transferred between the satellites and gateways per night. Figures of merit have been derived that offer insights into the performance for both an individual gateway and a network of gateways. Specific results are provided for the hypothetical gateway network, defined in Section 1, but the methods introduced here could be applied to understand performance of a different set of gateways.

The primary performance metric being investigated is the amount of secure key data that can be exchanged between satellites and gateways, as a function of the gateway location and the number of satellites in the constellation. Assuming that more key information is generally better, we would naturally aim for this; however good performance is more complex than this, depending on the objectives. For example, it might be the case where the maximum number of exchanged keys is

achieved when a large number of keys are exchanged between a small number of ground terminals and satellites; however, a more uniform spread of keys might be desirable across the network. Alternatively, should specific terminals have higher priority than others, it may be preferable for those terminals to receive more keys. This level of detail is application specific, such that the analysis here is kept intentionally generic. A uniform priority is assumed therefore, such that resource is distributed to gateways according to their relative availability.

Performance will be captured for each gateway (j) as a measure of the volume of shared key information per night for each month of the year (k). This is calculated as part of the simulation defined in the following section and is defined as follows:

$$k_j \approx \frac{x_j}{n}, \tag{6}$$

where x_j is the average volume of secure key data transferred per satellite per night to gateway j via a constellation of n satellites. This is based on the assumption that communication can only be between a single satellite–gateway pair (i.e., the satellite cannot transmit data to more than one gateway at any one time) and assumes that the influence of each satellite in the network on each of the gateways is similar. This latter assumption is considered acceptable given the close proximity of the gateways relative to the field of view from the satellites.

Using the above figure of merit means that, for this particular infrastructure, it is possible to understand the volume of key data that can be exchanged with gateways at different locations across the UK for different months through the year as a function of the number of satellites in the constellation. Indeed, a natural limitation exists due to the fact that there are only so many dark hours during the night, i.e., the maximum number of keys would be reached should there always be a satellite available for key transfer.

As well as the number of satellites in the constellation (n), the number of gateways being targeted (m) has a significant impact on the performance for each gateway independently. To generalise the problem, the relative transfer volume (maximum theoretical volume of key data per night) to each gateway in the network must be considered, such that the respective impact is proportional to this value. The secure key volume (V) delivered to gateway j during month k can thus be estimated as follows:

$$V_{j,k} \approx \frac{n v_{j,k}^2}{\sum_l^m v_{l,k}}, \tag{7}$$

where $v_{l,k}$ is the volume of data that could be transferred to gateway l during month k per satellite in the constellation. For example, consider a network of three gateways to which a key transfer capacity is considered as the potential to transfer data. For example, for a satellite that experienced two opportunities to transfer data to a gateway per day over which 20 MB and 10 MB could be transferred, respectively, the daily transfer capacity between these two nodes would be 30 MB. Ten, 5 and 0 per satellite per night can be attributed, respectively. Given a constellation of three satellites, gateway 1 would expect to receive 13.3 units per night, gateway 2 would expect to receive 3.3 units and gateway 3 would receive none. Effectively, this assumes that the available satellite resource is distributed to the gateways in a manner that is proportional to their respective potential transfer volume.

6.1. Model definition

Analysis of the QUARC mission performance (secure key transfer capacity) has been achieved through execution of a high-level numerical simulation model in combination with illumination and cloud-cover modelling (Figure 12). The simulation model considers the relative position of each satellite–gateway pair and outputs the elevation angle above the horizon for each step in the simulation. The simulation has a time-step duration of 10 seconds and represents 12 hours of real-time operations (between 18:00 hrs and 06:00 hrs).

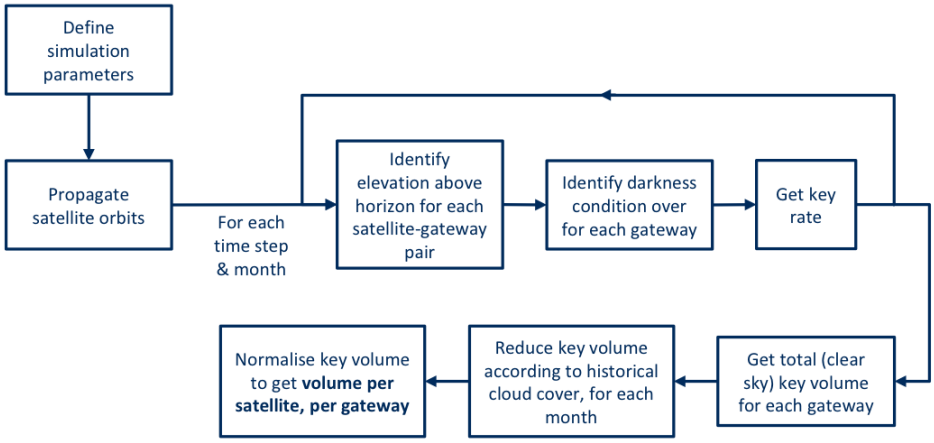

Figure 12. Simulation work flow.

The simulation results are combined with a sunrise–sunset model for the 15th day of each month of the year to establish the rate of key transfer during each gateway pass and the nominal (clear sky) satellite–gateway secure key volume transfer capacity. This nominal key volume capacity for each monthly 12-hour period is scaled according to the expected level of cloud cover (e.g., 50% cloud cover would scale the key volume for that period by a factor of 0.5).

The result of this analysis process is an expected secure key volume per satellite per gateway location for each month throughout the year and is illustrated in Figure 13.

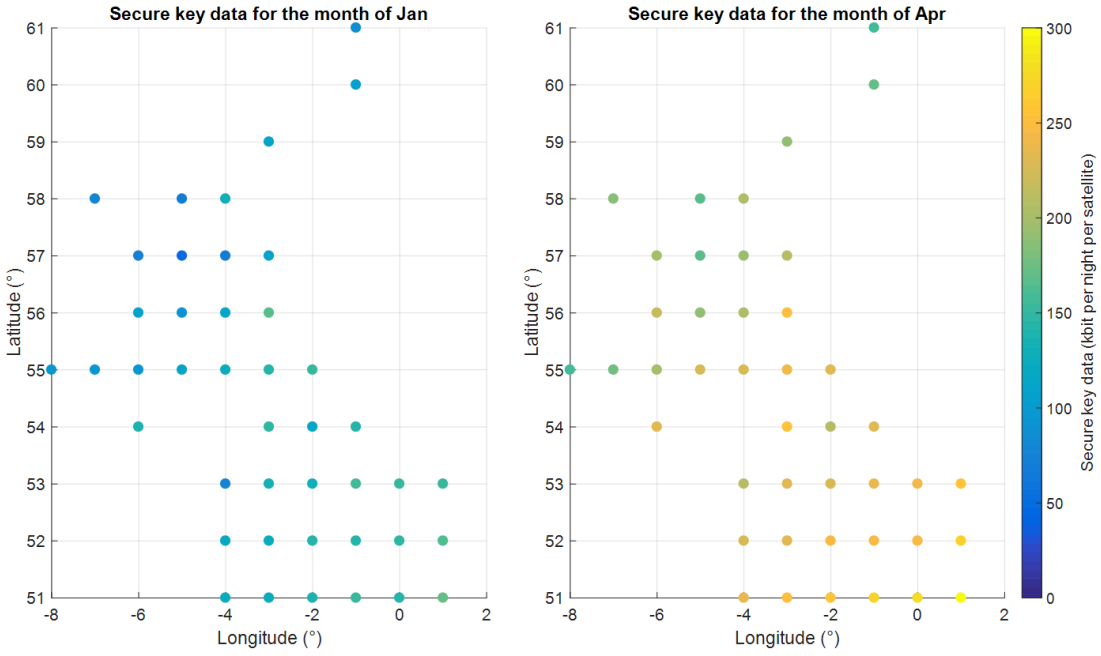

Figure 13. Key exchange during a typical January (left) and April (right).

6.2. Single Gateway Results

The results shown in Figures 13 and 14 illustrate the volume of secure key transfer to each gateway per night per satellite in the constellation for the months of January, April, June and September. It is important to note that these results show a hypothetical scenario for each gateway independent of all the others, i.e., assuming no other gateway is demanding satellite resource. This enables an insight into each gateway's relative capacity.

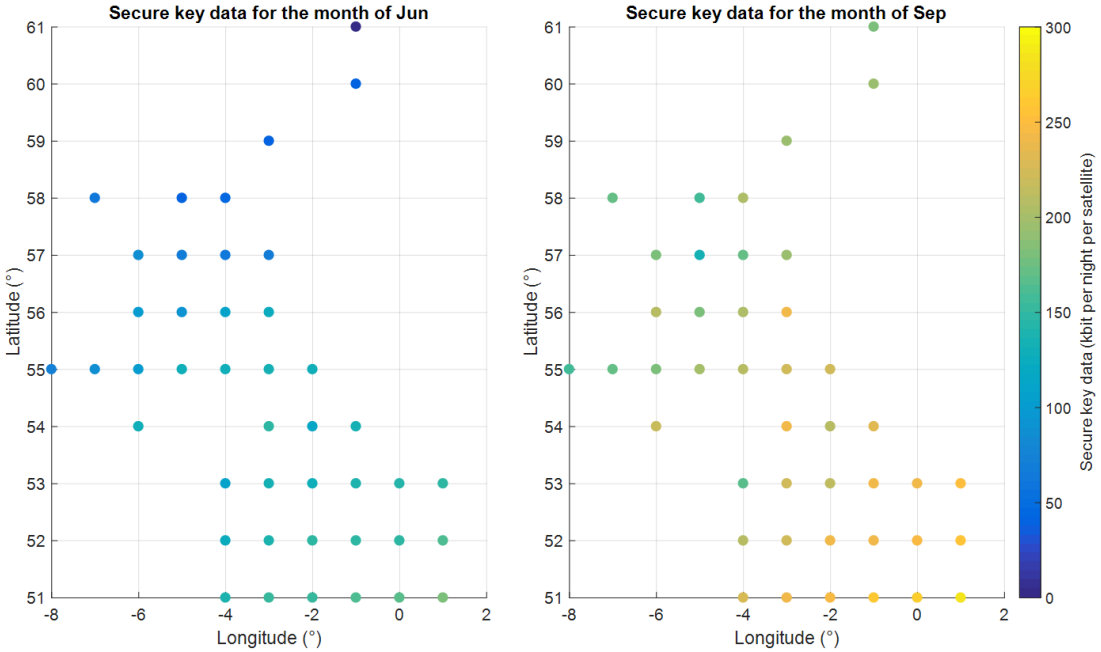

Figure 14. Key exchange during a typical June (left) and September (right).

From the above results, the variation in performance between different locations over the year is not straight forward. It is a complex coupling of dark sky duration, expected cloud coverage and satellite visibility. In general, the volume of secure key data transfer is greater during spring and autumn than in summer and winter. This can be attributed to significantly longer days in the summer months and significantly greater cloud coverage during winter months. Some locations exhibit uncharacteristically good performance compared to their surrounding regions, such as the east coast of Scotland (Lat 56°, Lon −3°) during the month of September.

6.3. Scaling for a Specific Gateway Topology

In the case where all 43 hypothetical gateways are demanding of resources from the 15 satellites, the resources are modelled as being shared according to each gateway's data-transfer capacity. Results are presented, again for January and April (Figure 15) and for June and September (Figure 16), showing the volume of secure key data that would be expected at each of the gateway locations per satellite in the constellation. Of course, in reality, operational requirements might demand a different distribution of resources, such that this approach can be seen as one particular use case.

While similar trends are seen in the results shown in the previous section, the variability in the transfer capacity is exaggerated due to the provision of data-transfer resources relative to communication capacity. This should be expected since more resources are applied to the gateways with greater transfer capacity in order to maximise the data transfer during times of high availability.

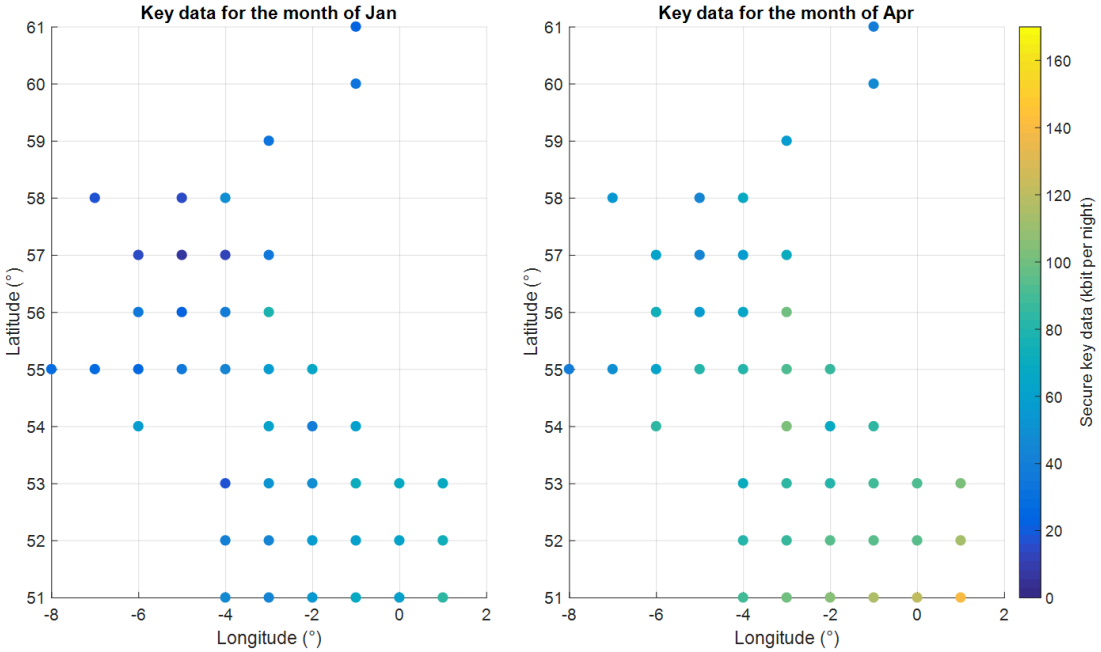

Figure 15. Mission total key exchange during a typical January (left) and April (right).

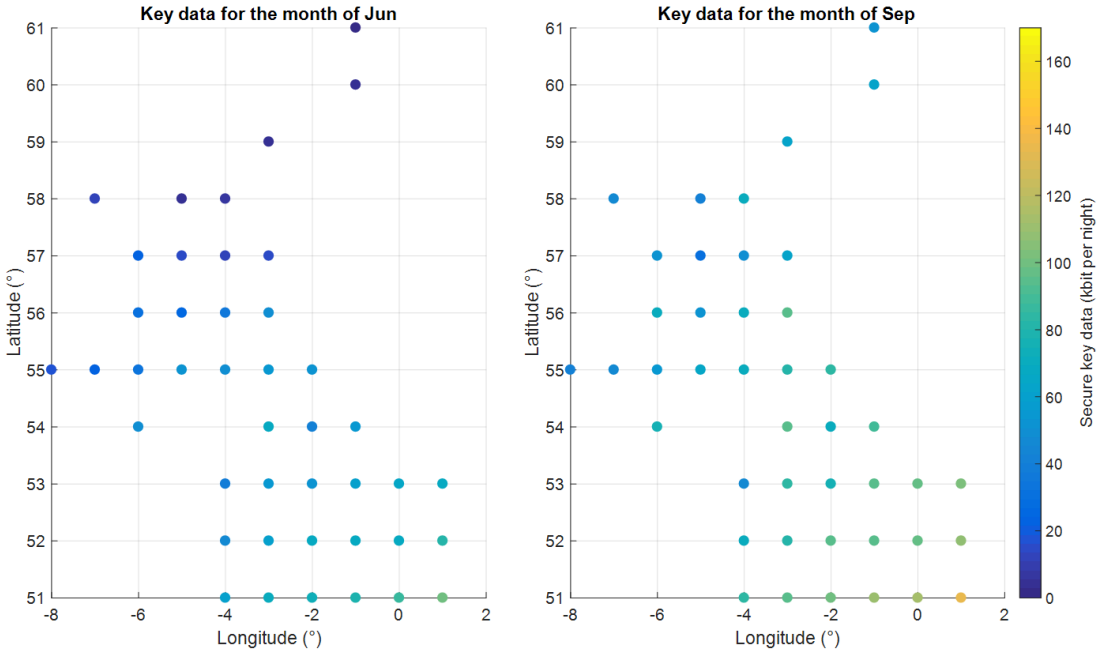

Figure 16. Mission total key exchange during a typical June (left) and September (right).

6.4. Time scale and budget considerations

COTS 700-mm aperture telescope systems for satellite optical communications are available for USD 200K [63,64]. With additional costs for the quantum receiver hardware and housing structure, a single OGS should cost less than USD 500K. The cost for the QKD ground segment could be considerably reduced by colocating SatQKD and conventional satellite laser communication infrastructure, i.e., utilising the same telescope for both operations. The main areas of payload development are source miniaturisation, ruggedization and security hardening; timing and

synchronisation systems; thermal design and analysis; design and manufacture of transmission telescope optics; and space-qualified software. A reasonable time scale for the development of this is 24 months given sufficient resources, and we envisage a recurring cost per CubeSat of around USD 500K (USD 300K platform, USD 100K optics and USD 100K other payload systems).

Launch costs are variable depending on whether a suitable rideshare opportunity into the desired orbits is available. Conservatively, we will assume a dedicated launch on a small rocket such as Rocket Lab's Electron which can put 220 kg into Sun synchronous orbit for USD5M [76]. The cost to deploy the constellation can thus be conservatively evaluated at USD25M assuming five separate launches, placing three 6U CubeSats into each orbital plane. Considering the capacity of the electron launcher (220 kg) and taking into account deployment container mass, each launch could place up to 15 6U CubeSats per orbital plane, which would greatly increase constellation capacity and would provide in-orbit redundancy. Alternatively plane-change manoeuvres could be achieved through raising or lowering the orbit altitude and by relying on a shift in right ascension of the ascending node through Earth's oblateness effects. While this approach is cost effective regarding launch, it requires time and propellant and adds an additional risk to the mission success. Once development is concluded, the deployment could be achieved in about 12 months (6 months assembly, integration and test of the payload/satellite, together with 6 months for integration with the launch vehicle and launch operations). These time and budget estimates indicate that a CubeSat constellation for QKD is in reach and can be developed within the framework of currently available technology.

The above results provide insights into the amount of secure key data that can be transferred to a UK-based ground network via a 15-platform CubeSat constellation. Indeed, operational and geographical constraints will play a significant part in real-world performance, which should be considered carefully in future studies. This can only be evaluated fully on a case-by-case basis, but the general approach and figures of merit defined in this work should offer a good starting point.

7. Conclusions

In this work, we have analysed the QUARC mission concept for a nanosatellite constellation to provide the UK with a satellite-based QKD capability. Due to the relatively low cost of CubeSats compared to traditional, large satellite platforms, deploying a large number of platforms may offer greater coverage which would mitigate some of the risk associated with performance limitations linked to cloud cover. Satellite constellations will also offer greater flexibility than a single platform when it is required to accommodate the communication demand of the underlying gateway network. Satellite-based QKD for securing critical infrastructure is of current interest with the launch of the EC-ESA Quantum Communication Infrastructure (QCI) initiative [77] that will require a space segment for continental-scale secure networks [78]. The UK is also pursuing CubeSat-based efforts to accelerate SatQKD as part of the National Quantum Technology Programme [37], and QUARC provides preliminary mission and performance analyses that will inform future developments.

An example mission topology has been presented, which includes a ground network of 43 gateways (to represent a large UK-infrastructure project) and a 15-satellite constellation. The satellites are placed into 574-km circular orbits, which are both Sun and Earth synchronous in order to ensure good coverage over the UK and consistent passes at useful times overnight.

A QKD payload and its performance have been modelled and tested to provide input for the secret key rate as a function of elevation. We have chosen trusted node QKD in order to reflect near-term realizability. Conservatively, we have assumed nighttime operation only. Operation during twilight hours may be possible with a reduction in key rate, thus extending the times at which key distribution could be performed.

In order to evaluate the secret key volume, we have developed a comprehensive channel simulation incorporating orbital propagation for the satellite constellation, twilight duration, losses, spurious event source as well as historical weather data. Our results show that a CubeSat constellation has the potential to deliver a small but reliable amount of secret key that could be used in

scenarios where highly secure communication is required, such as critical infrastructure management. Performance at specific gateway locations is shown to be highly dependent on geographical position and seasonal conditions. It is found that, in general, southern regions offer a more consistent long-term average rate of key transfer but with isolated regions further north benefiting from long overnight dark periods and minimal cloud cover during some winter months. The mission analysis results presented offer indicative levels of performance for gateways distributed across the UK; however, it is recommended that mission-specific analysis be carried out for different topologies [41].

Furthermore, our finding suggests that payloads optimised for operation with high background levels of light may be beneficial to extend coverage at high latitudes during the summer months, e.g., 1550-nm operation and aggressive temporal, spatial and spectral filtering. A shift toward 1550 nm would be also desirable in order to implement intersatellite links [42–45]. This may however compromise peak key distribution rates; hence, further studies will be needed to perform optimisation across payload and mission parameters coupled with a detailed key-demand and network-usage model including key buffering and refresh rates.

Author Contributions: Conceptualization, D.K.L.O. and L.M.; methodology, D.K.L.O. and L.M.; software, C.L. and L.M.; data curation C.L., D.L., S.K.J. and L.M.; validation S.G., D.M. and C.M.; writing—original draft preparation, L.M., C.L., S.K.J., D.L. and D.K.L.O.; writing—review and editing, L.M., C.L., S.K.J., D.L. and D.K.L.O.; supervision, D.K.L.O.; project administration, D.K.L.O.; funding acquisition, J.R., M.M. and D.K.L.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the UK Space Agency through the National Space Technology Programme (NSTP3-FT-063 "Quantum Research CubeSat", NSTP Fast Track "System Integration & Testing of a CubeSat WCP QKD Payload to TRL5"), EPSRC Quantum Technology Hub in Quantum Communication Partnership Resource (EP/M013472/1) and Innovate UK (EP/S000364/1). DKLO is supported by the EPSRC Researcher in Residence programme (EP/T517288/1), DKLO and LM acknowledge the travel support by the EU COST action QTSpace (CA15220), and LM acknowledges the travel support by Scottish Universities Physics Alliance SUPA (LC17683).

Acknowledgments: DKLO and LM acknowledges discussions with Alex Ling, Andy Vick, Thomas Jennewein, Erik Kerstel, Giuseppe Vallone, Paolo Villoresi and Harald Weinfurter.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ADCS	attitude determination and control system
APD	avalanche photo-diode
AOI	area of interest
APT	acquisition, pointing and tracking
BTC	beacon tracking camera
COTS	commercial, off-the-shelf
DCR	dark count rate
DL	downlink
FoV	field of view
FSM	fast steering mirror
LEO	low earth orbit
LoS	line-of-sight
MEMS	micro-electromechanical system
MM	micro-electromechanical system micromirror
OGS	optical ground station
PID	proportional-integral-differential
QBER	quantum bit error rate
QE	quantum efficiency

QKD	Quantum key distribution
QRNG	quantum random number generator
QUARC	quantum research CubeSat
RF	radio frequency
SatQKD	satellite quantum key distribution
SNSPD	superconducting nanowire single photon detector
SWaP	size, weight and power
UL	uplink

References

1. Bos, J.W.; Halderman, J.A.; Heninger, N.; Moore, J.; Naehrig, M.; Wustrow, E. Elliptic curve cryptography in practice. In *Financial Cryptography and Data Security*; Christin, N., Safavi-Naini, R., Eds.; Springer: Berlin, Germany, 2014; Volume 8437, pp. 157–175.
2. Alagic, G.; Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Liu, Y.K.; Miller, C.; Moody, D.; Peralta, R.; et al. *Status Report on the First Round of the NIST Post-quantum Cryptography Standardization Process*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
3. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
4. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. doi:10.1103/RevModPhys.81.1301. [CrossRef]
5. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. doi:10.1103/RevModPhys.74.145. [CrossRef]
6. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Wallden, P. Advances in Quantum Cryptography. *arXiv* **2019**. arXiv:1906.01645.
7. Azuma, K.; Tamaki, K.; Lo, H.K. All-photonic quantum repeaters. *Nat. Commun.* **2015**, *6*, 6787. doi:10.1038/ncomms7787. [CrossRef] [PubMed]
8. Donaldson, R.; Mazzarella, L.; Collins, R.; Jeffers, J.; Buller, G. A high-gain and high-fidelity coherent state comparison amplifier. *Comm. Phys.* **2018**, *1*, 54. [CrossRef]
9. Donaldson, R.J.; Mazzarella, L.; Zanforlin, U.; Collins, R.J.; Jeffers, J.; Buller, G.S. Quantum state correction using a measurement-based feedforward mechanism. *Phys. Rev.* **2019**, *100*, 023840. doi:10.1103/PhysRevA.100.023840. [CrossRef]
10. Wootters, W.; Zurek, W. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
11. Pandey, S.; Jiang, Z.; Combes, J.; Caves, C.M. Quantum limits on probabilistic amplifiers. *Phys. Rev.* **2013**, *88*, 033852. doi:10.1103/PhysRevA.88.033852. [CrossRef]
12. Bedington, R.; Arrazola, J.; Ling, A. Progress in satellite quantum key distribution. *NPJ Quantum Inf.* **2017**, *3*, 30. [CrossRef]
13. Khan, I.; Heim, B.; Neuzner, A.; Marquardt, C. Satellite-Based QKD. *Opt. Photonics News* **2018**, *29*, 26–33. doi:10.1364/OPN.29.2.000026. [CrossRef]
14. Moll, F.; Botter, T.; Marquardt, C.; Pusey, D.; Shrestha, A.; Reeves, A.; Jaksch, K.; Gunthner, K.; Bayraktar, O.; Mueller-Hirschkorn, C.; et al. Stratospheric QKD: feasibility analysis and free-space optics system concept. In *Quantum Technologies and Quantum Information Science V*; Gruneisen, M.T., Dusek, M., Alsing, P.M., Rarity, J.G., Eds.; International Society for Optics and Photonics: San Francisco, CA, USA, 2019; Volume 11167, pp. 34–42. doi:10.1117/12.2539076. [CrossRef]
15. Agnesi, C.; Vedovato, F.; Schiavon, M.; Dequal, D.; Calderaro, L.; Tomasin, M.; Marangon, D.G.; Stanco, A.; Luceri, V.; Bianco, G.; et al. Exploring the boundaries of quantum mechanics: advances in satellite quantum communications. *Philos. Trans. Royal Soc. A* **2018**, *376*, 20170461. doi:10.1098/rsta.2017.0461. [CrossRef] [PubMed]

16. Bourgoin, J.P.; Meyer-Scott, E.; Higgins, B.L.; Helou, B.; Erven, C.; Habel, H.; Kumar, B.; Hudson, D.; D'Souza, I.; Girard, R.; et al. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New J. Phys.* **2013**, *15*, 023006. doi:10.1088/1367-2630/15/2/023006. [CrossRef]
17. Kimble, H.J. The quantum internet. *Nature* **2008**, *453*, 1023–1030. doi:10.1038/nature07127. [CrossRef]
18. Vergoossen, T.; Loarte, S.; Bedington, R.; Kuiper, H.; Ling, A. Satellite constellations for trusted node QKD networks. *arXiv* **2019**, arXiv:1903.07845.
19. Vallone, G.; Bacco, D.; Dequal, D.; Gaiarin, S.; Luceri, V.; Bianco, G.; Villoresi, P. Experimental Satellite Quantum Communications. *Phys. Rev. Lett.* **2015**, *115*, 040502. doi:10.1103/PhysRevLett.115.040502. [CrossRef]
20. Günthner, K.; Khan, I.; Elser, D.; Stiller, B.; Ömer Bayraktar.; Müller, C.R.; Saucke, K.; Tröndle, D.; Heine, F.; Seel, S.; et al. Quantum-limited measurements of optical signals from a geostationary satellite. *Optica* **2017**, *4*, 611–616. doi:10.1364/OPTICA.4.000611. [CrossRef]
21. Pugh, C.J.; Kaiser, S.; Bourgoin, J.P.; Jin, J.; Sultana, N.; Agne, S.; Anisimova, E.; Makarov, V.; Choi, E.; Higgins, B.L.; et al. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Sci. Technol.* **2017**, *2*, 024009. doi:10.1088/2058-9565/aa701f. [CrossRef]
22. Dequal, D.; Vallone, G.; Bacco, D.; Gaiarin, S.; Luceri, V.; Bianco, G.; Villoresi, P. Experimental single-photon exchange along a space link of 7000 km. *Phys. Rev.* **2016**, *93*, 010301. doi:10.1103/PhysRevA.93.010301. [CrossRef]
23. Nauerth, S.; Moll, F.; Rau, M.; Fuchs, C.; Horwath, J.; Frick, S.; Weinfurter, H. Air-to-ground quantum communication. *Nat. Photonics* **2013**, *7*, 382–386. doi:10.1038/nphoton.2013.46. [CrossRef]
24. Wang, J.Y.; Yang, B.; Liao, S.K.; Zhang, L.; Shen, Q.; Hu, X.F.; Wu, J.C.; Yang, S.J.; Jiang, H.; Tang, Y.L.; et al. Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nat. Photonics* **2013**, *7*, 387–393. doi:10.1038/nphoton.2013.89. [CrossRef]
25. James A. Grieve and Robert Bedington and Zhongkan Tang and Rakhitha C.M.R.B. Chandrasekara and Alexander Ling. SpooQySats: CubeSats to demonstrate quantum key distribution technologies. *Acta Astronaut.* **2018**, *151*, 103–106. doi:{https://doi.org/10.1016/j.actaastro.2018.06.005}. [CrossRef]
26. Yin, J.; Cao, Y.; Li, Y.H.; Liao, S.K.; Zhang, L.; Ren, J.G.; Cai, W.Q.; Liu, W.Y.; Li, B.; Dai, H.; et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **2017**, *356*, 1140–1144. doi:10.1126/science.aan3211. [CrossRef] [PubMed]
27. Vedovato, F.; Agnesi, C.; Schiavon, M.; Dequal, D.; Calderaro, L.; Tomasin, M.; Marangon, D.G.; Stanco, A.; Luceri, V.; Bianco, G.; et al. Extending Wheeler's delayed-choice experiment to space. *Sci. Adv.* **2017**, *3*, e1701180. doi:10.1126/sciadv.1701180. [CrossRef] [PubMed]
28. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. doi:10.1038/nature23655. [CrossRef] [PubMed]
29. Yin, J.; Cao, Y.; Li, Y.H.; Ren, J.G.; Liao, S.K.; Zhang, L.; Cai, W.Q.; Liu, W.Y.; Li, B.; Dai, H.; et al. Satellite-to-Ground Entanglement-Based Quantum Key Distribution. *Phys. Rev. Lett.* **2017**, *119*, 200501. doi:10.1103/PhysRevLett.119.200501. [CrossRef]
30. Liao, S.K.; Cai, W.Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.G.; Liu, W.Y.; et al. Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.* **2018**, *120*, 030501. doi:10.1103/PhysRevLett.120.030501. [CrossRef]
31. European Space Agency. D/TIA partners with UK-based ArQit to develop first Quantum Encryption Satellite. 2018. Available online: https://artes.esa.int/news/dtia-partners-uk-based-arqit-develop-first-quantum-encryption-satellite (accessed on 21 December 2019).
32. European Space Agency. 10 new business and research partners join Quartz. 2018. Available online: https://artes.esa.int/news/10-new-business-and-research-partners-join-quartz (accessed on 21 December 2019).
33. Jennewein, T.; Bourgoin, J.P.; Higgins, B.; Holloway, C.; Meyer-Scott, E.; Erven, C.; Heim, B.; Yan, Z.; Hübel, H.; Weihs, G.; et al. QEYSSAT: a mission proposal for a quantum receiver in space. In Proceedings of the Advances in Photonics of Quantum Computing, Memory, and Communication VII; Hasan, Z.U., Hemmer, P.R., Lee, H., Santori, C.M., Eds.; International Society for Optics and Photonics: San Francisco, CA, USA, 2014; Volume 8997, pp. 21–27. doi:10.1117/12.2041693. [CrossRef]

34. Department for Business, Energy and Industrial Strategy, United Kingdom. UK and Singapore come together to launch £10m Quantum Space Programme. 2019. Available online: https://www.gov.uk/government/news/uk-and-singapore-come-together-to-launch-10m-quantum-space-programme (accessed on 21 December 2019).
35. Haber, R.; Garbe, D.; Busch, S.; Rosenfeld, W.; Schilling, K. Qube - A CubeSat for Quantum Key Distribution Experiments. 2018. Available online: https://digitalcommons.usu.edu/smallsat/2018/all2018/269/ (accessed on 10 February 2020).
36. Kerstel, E.; Gardelein, A.; Barthelemy, M.; Fink, M.; Joshi, S.K.; Ursin, R.; Team, T.C. Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technol.* **2018**, *5*, 6. doi:10.1140/epjqt/s40507-018-0070-7. [CrossRef]
37. UK National Quantum Technologies Programme. Space-based quantum security. 2019. Available online: http://uknqt.epsrc.ac.uk/files/spacebasedquantumsecurity/ (accessed on 21 December 2019).
38. Oi, D.K.; Ling, A.; Vallone, G.; Villoresi, P.; Greenland, S.; Kerr, E.; Macdonald, M.; Weinfurter, H.; Kuiper, H.; Charbon, E.; et al. CubeSat quantum communications mission. *EPJ Quantum Technol.* **2017**, *4*, 6. doi:10.1140/epjqt/s40507-017-0060-1. [CrossRef]
39. Oi, D.K.L.; Ling, A.; Grieve, J.A.; Jennewein, T.; Dinkelaker, A.N.; Krutzik, M. Nanosatellites for quantum science and technology. *Contemp. Phys.* **2017**, *58*, 25–52. doi:10.1080/00107514.2016.1235150. [CrossRef]
40. Tysowski, P.K.; Ling, X.; Lütkenhaus, N.; Mosca, M. The Engineering of a Scalable Multi-Site Communications System Utilizing Quantum Key Distribution (QKD). *Quantum Sci. Technol.* **2017**, *3*, 024001. doi:10.1088/2058-9565/aa9a5d. [CrossRef]
41. Polnik, M.; Mazzarella, L.; Di Carlo, M.; Oi, D.K.; Riccardi, A.; Arulselvan, A. Scheduling of space to ground quantum key distribution. *EPJ Quantum Technol.* **2020**, *7*, 3. doi:10.1140/epjqt/s40507-020-0079-6. [CrossRef]
42. Naughton, D.P.; Bedington, R.; Barraclough, S.; Islam, T.; Griffin, D.; Smith, B.; Kurtz, J.; Alenin, A.S.; Vaughn, I.J.; Ramana, A.; et al. Design considerations for an optical link supporting intersatellite quantum key distribution. *Opt. Eng.* **2019**, *58*, 1 – 13. doi:10.1117/1.OE.58.1.016106. [CrossRef]
43. Ko, H.; Kim, K.J.; Choe, J.S.; Choi, B.S.; Kim, J.H.; Baek, Y.; Youn, C.J. Experimental filtering effect on the daylight operation of a free-space quantum key distribution. *Sci. Rep.* **2018**, *8*, 15315. doi:10.1038/s41598-018-33699-y. [CrossRef]
44. Liao, S.K.; Yong, H.L.; Liu, C.; Shentu, G.L.; Li, D.D.; Lin, J.; Dai, H.; Zhao, S.Q.; Li, B.; Guan, J.Y.; et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photon.* **2017**, *11*, 509–513. doi:10.1038/nphoton.2017.116. [CrossRef]
45. Avesani, M.; Calderaro, L.; Schiavon, M.; Stanco, A.; Agnesi, C.; Santamato, A.; Zahidy, M.; Scriminich, A.; Foletto, G.; Contestabile, G.; et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *arXiv* **2019**, arXiv:1907.10039. Available online: https://arxiv.org/pdf/1907.10039.pdf (accessed on 10 February 2020).
46. Bonnetain, X.; Naya-Plasencia, M.; Schrottenloher, A. Quantum Security Analysis of AES. *IACR Trans. Symm. Cryptol.* **2019**, *2019*, 55–93. doi:10.13154/tosc.v2019.i2.55-93. [CrossRef]
47. Neumann, S.P.; Joshi, S.K.; Fink, M.; Scheidl, T.; Blach, R.; Scharlemann, C.; Abouagaga, S.; Bambery, D.; Kerstel, E.; Barthelemy, M.; et al. Q3Sat: quantum communications uplink to a 3U CubeSat—feasibility & design. *EPJ Quantum Technol.* **2018**, *5*, 4. doi:10.1140/epjqt/s40507-018-0068-1. [CrossRef]
48. Mélen, G.; Freiwang, P.; Luhn, J.; Vogl, T.; Rau, M.; Rosenfeld, W.; Weinfurter, H. Handheld Quantum Key Distribution. In Proceedings of the 2018 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 13–18 May 2018.
49. Lowndes, D.; Frick, S.; Harrington, B.; Rarity, J. Low Cost, Short Range Quantum Key Distribution. In Proceedings of the 2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), Munich, Germany, 25–29 June 2017.
50. Gagliardi, R.M.; Karp, S. *Optical Communications*; Wiley-Interscience: New York, NY, USA, 1976.
51. Vasylyev, D.; Vogel, W.; Moll, F. Satellite-mediated quantum atmospheric links. *Phys. Rev.* **2019**, *99*, 053830. doi:10.1103/PhysRevA.99.053830. [CrossRef]
52. Sibson, P.; Kennard, J.E.; Stanisic, S.; Erven, C.; O'Brien, J.L.; Thompson, M.G. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **2017**, *4*, 172–177. doi:10.1364/OPTICA.4.000172. [CrossRef]

53. Bacco, D.; Ding, Y.; Dalgaard, K.; Rottwitt, K.; Oxenløwe, L.K. Space division multiplexing chip-to-chip quantum key distribution. *Sci. Rep.* **2017**, *7*, 12459. doi:10.1038/s41598-017-12309-3. [CrossRef] [PubMed]
54. Canning, D.W.; Donaldson, R.J.; Mukherjee, S.; Collins, R.J.; Mazzarella, L.; Zanforlin, U.; Jeffers, J.; Thomson, R.R.; Buller, G.S. On-chip implementation of the probabilistic quantum optical state comparison amplifier. *Optic. Express* **2019**, *27*, 31713–31726. doi:10.1364/OE.27.031713. [CrossRef] [PubMed]
55. Vest, G.; Rau, M.; Fuchs, L.; Corrielli, G.; Weier, H.; Nauerth, S.; Crespi, A.; Osellame, R.; Weinfurter, H. Design and Evaluation of a Handheld QuantumKey Distribution Sender module. *IEEE J. Sel. Top. Quant. Electron.* **2015**, *21*, 131–137. doi:10.1109/JSTQE.2014.2364131. [CrossRef]
56. Andrews, L.C.; Phillips, R.L. Laser Beam Propagation Through Random Media. SPIE digital library: Bellingham, WA, USA, 2005. doi:10.1117/3.626196. [CrossRef]
57. Boaron, A.; Korzh, B.; Houlmann, R.; Boso, G.; Rusca, D.; Gray, S.; Li, M.J.; Nolan, D.; Martin, A.; Zbinden, H. Simple 2.5GHz time-bin quantum key distribution. *Appl. Phys. Lett.* **2018**, *112*, 171108. doi:10.1063/1.5027030. [CrossRef]
58. Herrero-Collantes, M.; Garcia-Escartin, J.C. Quantum random number generators. *Rev. Mod. Phys.* **2017**, *89*, 015004. [CrossRef]
59. Mirrorcle Technologies Inc., Mirrorcle S40069. Available online: https://www.mirrorcletech.com/devices.html (accessed on 10 February 2020).
60. Mazzarella, L.; Donaldson, R.J.; Collins, R.J.; Zanforlin, U.; Tatsi, G.; Buller, G.S.; Jeffers, J. Quantum state comparison amplifier with feedforward state correction. In *Quantum Technologies 2018*; Stuhler, J., Shields, A.J., Padgett, M.J., Eds.; International Society for Optics and Photonics: San Francisco, CA, USA, 2018, Volume 10674, pp. 153–161. doi:10.1117/12.2307818. [CrossRef]
61. Uysal, M.; Capsoni, C.; Ghassemlooy, Z.; Boucouvalas, A.; Udvary, E. *Optical Wireless Communications: An Emerging Technology*; Springer International Publishing: Berlin, Germany, 2016.
62. Fuchs, C.; Kolev, D.; Moll, F.; Shrestha, A.; Brechtelsbauer, M.; Rein, F.; Schmidt, C.; Akioka, M.; Munemasa, Y.; Takenaka, H.; et al. Sota optical downlinks to DLR's optical ground stations. In Proceedings of the International Conference on Space Optics – ICSO 2016, Cugny, Biarritz, France, 25 September 2017; Volume 10562, pp. 1228–1236. doi:10.1117/12.2296107. [CrossRef]
63. PlaneWave Instruments Inc.. CDK700 (0.7M CDK TELESCOPE SYSTEM). 2020. Available online: http://pw-ecommerce.com/product/cdk700-0-7m-cdk-telescope-system/ (accessed on 10 February 2020).
64. PlaneWave Instruments Inc. Laser Communications and Space Situational Awareness Applications. 2020. Available online: https://www.planewave.eu/en/planewave-europe/space-applications (accessed on 10 February 2020).
65. Kaushal, H.; Kaddoum, G. Free Space Optical Communication: Challenges and Mitigation Techniques. *arXiv* **2015**, arXiv:1506.04836. Available online: https://arxiv.org/pdf/1506.04836.pdf (accessed on 10 February 2020).
66. Berk, A.; Conforti, P.; Kennett, R.; Perkins, T.; Hawes, F.; van den Bosch, J. MODTRAN6: a major upgrade of the MODTRAN radiative transfer code. In Proceedings of the 6th Workshop on Hyperspectral Image and Signal Processing: Evolution in Remote Sensing (WHISPERS), Lausanne, Switzerland, 24–27 June 2014; Volume 9088, pp. 113–119. doi:10.1117/12.2050433. [CrossRef]
67. Hills, M.J.; Bradshaw, T.W.; Dobrovolskiy, S.; Dorenbos, S.N.; Gemmell, N.R.; Green, B.; Heath, R.M.; Rawlings, T.; Tsimvrakidis, K.; Zwiller, V.; et al. A compact 4 K cooling system for superconducting nanowire single photon detectors. In Proceedings of the 27th International Cryogenics Engineering Conference and International Cryogenic Materials Conference 2018 (ICEC-ICMC 2018), Oxford, UK, 3–7 September 2018; Volume 502, pp. 012193. doi:10.1088/1757-899x/502/1/012193. [CrossRef]
68. Eso SkyCalc Web Application. Available online: https://www.eso.org/observing/etc/doc/skycalc/helpskycalc.html (accessed on 10 February 2020).
69. Mendoza, G.J.; Santagati, R.; Munns, J.; Hemsley, E.; Piekarek, M.; Martín-López, E.; Marshall, G.D.; Bonneau, D.; Thompson, M.G.; O'Brien, J.L. Active temporal and spatial multiplexing of photons. *Optica* **2016**, *3*, 127–132. doi:10.1364/OPTICA.3.000127. [CrossRef]
70. Mazzarella, L.; Ticozzi, F.; Sergienko, A.V.; Vallone, G.; Villoresi, P. Asymmetric architecture for heralded single-photon sources. *Phys. Rev.* **2013**, *88*, 023848. doi:10.1103/PhysRevA.88.023848. [CrossRef]
71. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. doi:10.1103/PhysRevLett.94.230504. [CrossRef]

72. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev.* **2005**, *72*, 012326. doi:10.1103/PhysRevA.72.012326. [CrossRef]
73. Met Office, Department for Business, Energy and Industrial Strategy, United Kingdom. How we measure cloud. 2019. Available online: https://www.metoffice.gov.uk/guide/weather/observations-guide/how-we-measure-cloud (accessed on 4 March 2019).
74. Morf, H. Sunshine and cloud cover prediction based on Markov processes. *Sol. Energ.* **2014**, *110*, 615–626. [CrossRef]
75. Met Office, Department for Business, Energy and Industrial Strategy, United Kingdom. Data: Access to UK climate datasets. 2019. Available online: https://www.metoffice.gov.uk/research/climate/maps-and-data/data/index (accessed on 21 December 2019).
76. Lab, R. Rocket Lab's 1st launch of 2020 is for the National Reconnaissance Office, the US spysat agency. 2020. Available online: https://www.space.com/rocket-lab-to-launch-nro-spy-satellite-january-2020.html (accessed on 10 February 2020).
77. European Commission. Nine More Countries Join Initiative to Explore Quantum Communication for Europe. 2020. Available online: https://ec.europa.eu/digital-single-market/en/news/nine-more-countries-join-initiative-explore-quantum-communication-europe (accessed on 10 February 2020).
78. Erman, M.; Vittadini, G.; Sanudo, J.-C.; Tschernitz, S.L.; Khan, I.; Tünnermann, A.; Vieira, I.; Vincente del Olmo, L.I.; Farwerck, J.; Molina, M.A.; et al. European Industry Whitepaper on the European Quantum Communication Infrastructure. 2020. Available online: http://www.qtspace.eu/sites/testqtspace.eu/files/other_files/IndustryWhitePaper_V3.pdf (accessed on 10 February 2020).